

CyberArk

Exam Questions CPC-SEN

CyberArk Sentry - Privilege Cloud



NEW QUESTION 1

Which statement is correct about using the AllowedSafes platform parameter?

- A. It allows users to access accounts in specific safes.
- B. It prevents the CPM from scanning all safes, restricting it to scan only safes that match the AllowedSafes configuration.
- C. It allows the CPM to access PSM safes to monitor platform configuration and connection component changes.
- D. It prevents the CPM from processing pending items in the Discovery safes enforcing manual intervention to complete the onboarding process.

Answer: B

Explanation:

The correct statement about using the AllowedSafes platform parameter is that it prevents the Central Policy Manager (CPM) from scanning all safes, restricting it to scan only safes that match the AllowedSafes configuration. This parameter is crucial in large-scale deployments where efficiency and resource management are key. By specifying which safes the CPM should manage, unnecessary scanning of irrelevant safes is avoided, thus optimizing the CPM's performance and reducing the load on the CyberArk environment. This configuration can be found in the platform management section of the CyberArk documentation.

NEW QUESTION 2

A support team has asked you to provide the previous password for an account that had its password recently changed by the CPM. In which tab within the account's overview page can you retrieve this information?

- A. Activities
- B. Details
- C. Versions

Answer: D

Explanation:

To retrieve the previous password for an account that had its password changed by the CPM, you should look under the Versions tab within the account's overview page. This tab maintains a history of password changes, including previous passwords, along with other historical data points that allow for tracking changes over time. This feature is critical for auditing and rollback purposes in environments where knowing past credentials is necessary for troubleshooting or compliance.

NEW QUESTION 3

How should you configure PSM for SSH to support load balancing?

- A. by using a network load balancer
- B. in PVWA > Options > PSM for SSH Proxy > Servers
- C. in PVWA > Options > PSM for SSH Proxy > Servers > VIP
- D. by editing sshd.config on the all the PSM for SSH servers

Answer: A

Explanation:

To support load balancing for PSM for SSH, the configuration should be done by using a network load balancer. This method involves placing a network load balancer in front of multiple PSM for SSH servers to distribute incoming SSH traffic evenly among them. This setup enhances the availability and scalability of PSM for SSH by ensuring that no single server becomes a bottleneck, thereby improving performance and reliability during high usage scenarios.

NEW QUESTION 4

During CPM hardening, which locally created users are granted Logon as a Service rights in the local group policy? (Choose 2.)

- A. PasswordManager
- B. PluginManagerUser
- C. ScannerUser
- D. PasswordManagerUser
- E. CPMSERVICEACCOUNT

Answer: AD

Explanation:

During the Central Policy Manager (CPM) hardening process, the locally created users that are granted 'Logon as a Service' rights in the local group policy are typically PasswordManager and PasswordManagerUser. These accounts are crucial for the CPM's operation as they handle password management tasks and require the ability to log on as a service to perform their functions effectively. This configuration is established to ensure that these service accounts can operate under service control manager without interruption, which is critical for automated password rotations and other security processes managed by the CPM. This detail is typically outlined in the CyberArk CPM installation and configuration guide.

NEW QUESTION 5

What are dependencies to update or change the CPM credential? (Choose 2.)

- A. APIKeyManager.exe
- B. CreateCredFile.exe
- C. CPM/nDomain_Hardening.ps1
- D. CyberArk.TPC.exe
- E. Data Execution Prevention

Answer: BD

Explanation:

To update or change the Central Policy Manager (CPM) credentials, dependencies include:

? CreateCredFile.exe (B): This utility is used to create or modify the encrypted file that stores the CPM's credentials. It is essential for securely handling the credential updates.

? CyberArk.TPC.exe (D): This executable is part of the CyberArk suite that manages trusted platform module operations, which can include tasks related to credential security and management, particularly when hardware security modules are involved.

NEW QUESTION 6

You plan to install Privilege Cloud Connectors on your AWS and Azure environments.

What is the maximum number of concurrent RDP/SSH sessions that each connector can handle for Large Implementations?

- A. 1-10
- B. 31-60
- C. 100
- D. 200

Answer: B

Explanation:

For large implementations of CyberArk Privilege Cloud Connectors in AWS and Azure environments, each connector can handle between 31-60 concurrent RDP/SSH sessions.

This capacity is specified in the CyberArk documentation concerning Privilege Cloud Connectors and their scalability options. It is designed to support a higher volume of concurrent sessions to meet the needs of larger enterprise environments, ensuring that multiple users can securely access resources without significant performance degradation.

NEW QUESTION 7

You are creating a PSM Load Balanced Virtual Server Configuration.

What are the default service ports / protocols used for RDS and the PSM Health Check service?

- A. RDP/389 HTTP/443
- B. RDP/3389 HTTPS/443
- C. UDP/53 HTTPS/389
- D. RDP/636 HTTPS/443

Answer: B

Explanation:

In a PSM Load Balanced Virtual Server Configuration, the default service ports/protocols used are RDP/3389 and HTTPS/443. RDP (Remote Desktop Protocol) typically uses port 3389 for remote desktop services, which is essential for PSM functionalities involving remote sessions. HTTPS, which utilizes port 443, is used for the PSM Health Check service to ensure secure and encrypted communication during the monitoring and health verification processes of the PSM services.

NEW QUESTION 8

You are implementing LDAPS Integration for a standard Privilege Cloud environment.

Which information must be provided to the CyberArk Privilege Cloud support team through a Service Request? (Choose 2.)

- A. LDAPS certificate chain for all domain controllers to be integrated
- B. LDAP bind username and password used to authenticate to the directory to be integrated
- C. Domain Base Context used to locate the users and groups in the Active Directory to be integrated
- D. Fully Qualified Domain Name and IP Address of the domain controllers to be integrated
- E. remote port set during secure tunnel configuration for each domain controller to be integrated

Answer: AD

Explanation:

When implementing LDAPS Integration for a standard Privilege Cloud environment, certain information is crucial and must be provided to the CyberArk Privilege Cloud support team through a Service Request. The necessary details include:

? LDAPS certificate chain for all domain controllers to be integrated (Option A): This

information is critical to establishing a trusted secure connection between the Privilege Cloud and the domain controllers using LDAP over SSL (LDAPS).

? Fully Qualified Domain Name and IP Address of the domain controllers to be

integrated (Option D): This information is essential for accurately identifying and configuring the network connections to each domain controller that will be integrated with the Privilege Cloud.

Reference: The process of setting up LDAPS integration typically requires detailed network and security information about the domain controllers to ensure secure and reliable connectivity. CyberArk support documentation and service request forms usually specify the need for these details.

NEW QUESTION 9

After correctly configuring reconciliation parameters in the Prod-AIX-Root-Accounts Platform, this error message appears in the CPM log: CACPM410E Ending password policy Prod-AIX-Root-Accounts since the reconciliation task is active but the AllowedSafes parameter was not updated What caused this situation?

- A. The reconciliation account defined in the Platform is in a locked state and is not accessible.
- B. The CPM is currently configured to use to an unsigned engine.
- C. The AllowedSafes parameter does not include the safe containing the reconciliation account defined in the Platform.
- D. A second CPM is incorrectly configured to manage the reconciliation account's safe which is causing a deadlock situation between the two CPMs.

Answer: C

Explanation:

The error message "CACPM410E Ending password policy Prod-AIX-Root-Accounts since the reconciliation task is active but the AllowedSafes parameter was not updated" suggests an issue with configuration parameters. The likely cause is:

? The AllowedSafes parameter does not include the safe containing the

reconciliation account defined in the Platform (Option C). This parameter must accurately reflect all safes where the reconciliation account operates to ensure

proper management and access by the Central Policy Manager (CPM). If the safe containing the reconciliation account is not listed, the CPM cannot perform its tasks, leading to this error.

Reference: CyberArk's error codes and troubleshooting guides detail how specific configuration mismatches, like an incomplete AllowedSafes parameter, can disrupt normal operations, especially in reconciliation processes.

NEW QUESTION 10

Which option correctly describes the authentication differences between CyberArk Privilege Cloud and CyberArk PAM Self-Hosted?

- A. CyberArk Privilege Cloud only provides a username and password authentication without third-party IdP integration; CyberArk PAM Self-Hosted uses traditional on-premises methods such as Windows and LDA
- B. but lacks modern protocols such as SAML or OIDC.
- C. CyberArk Privilege Cloud uses cloud-based methods, integrating with CyberArk Identity for MF
- D. and supports SAML and OIDC; CyberArk PAM Self-Hosted depends on on-premises methods such as RADIUS and LDAP, but can adopt SAML or OIDC with additional setups.
- E. CyberArk Privilege Cloud requires on-premises components for all authentication and does not support other cloud-based authentication protocols; CyberArk PAM Self-Hosted offers a wide array of methods, including support for SAM
- F. OID
- G. and other modern protocols, without needing on-premises components.
- H. Both use the same authentication methods.

Answer: B

Explanation:

The correct description of the authentication differences between CyberArk Privilege Cloud and CyberArk PAM Self-Hosted is that CyberArk Privilege Cloud uses cloud-based methods, integrating with CyberArk Identity for Multi-Factor Authentication (MFA), and supports SAML and OIDC, while CyberArk PAM Self-Hosted relies on on-premises methods such as RADIUS and LDAP, but can adopt SAML or OIDC with additional setups. CyberArk Privilege Cloud is designed to leverage modern cloud-based authentication protocols to enhance security and ease of use, particularly in distributed and diverse IT environments. In contrast, CyberArk PAM Self-Hosted offers flexibility to use traditional on-premises authentication methods but also supports modern protocols if configured to do so.

NEW QUESTION 10

Before the hardening process, your customer identified a PSM Universal Connector executable that will be required to run on the PSM. Which file should you update to allow this to run?

- A. PSMConfigureAppLocker.xml
- B. PSMHardening.xml
- C. PSMAppConfig.xml
- D. PSMConfigureHardening.xml

Answer: A

Explanation:

To allow a PSM Universal Connector executable to run on the PSM after the hardening process, you should update the PSMConfigureAppLocker.xml file. This file configures AppLocker, which is a feature that controls which apps and files users can run on a system. Including the necessary executable in the PSMConfigureAppLocker.xml ensures it is whitelisted by AppLocker policies, thus permitted to execute even under the hardened security settings of the PSM environment. References to this configuration can be found in the CyberArk Privilege Session Manager implementation documentation, specifically in sections detailing customization and security hardening of environment configurations.

NEW QUESTION 15

Which tool configures the user object that will be used during the installation of the PSM for SSH component?

- A. CreateUserPass
- B. CreateCredFile
- C. ConfigureCredFile
- D. ConfigureUserPass

Answer: B

Explanation:

The tool used to configure the user object for the installation of the PSM for SSH component is CreateCredFile. This tool is responsible for creating a credentials file that stores the necessary user details required during the installation process, ensuring secure and correct authentication.

References:

? CyberArk Privilege Cloud Introduction

NEW QUESTION 20

Refer to the exhibit.

You set up your LDAP Directory in CyberArk Identity, but encountered an error during the connection test.

Which scenarios could represent a valid misconfiguration? (Choose 2.)

Test Connection



Cannot contact the LDAP server. Possible causes of this error include: The transport connection to the LDAP server is not secured with SSL, the server running the connector does not trust the LDAP server's SSL certificate or the LDAP server is not reachable on the specified port (636 if not specified).

Close

- A. TCP Port 636 could be blocked by a network firewall, preventing communication between the CyberArk Identity Connector and the LDAP Server.
- B. All required CA Certificates have been installed on the CyberArk Identity Connector but the LDAP Bind credentials provided are incorrect.
- C. 'Verify Server Certificate' is activated but the provided hostname is not listed as a Subject Alternative Name (SAN) in the LDAP server's certificate.
- D. TCP Port 636 could be blocked by a network firewall, preventing communication between the Secure Tunnel and the LDAP Server.

Answer: AC

Explanation:

From the error message provided, two likely scenarios could represent valid misconfigurations:

? TCP Port 636 could be blocked by a network firewall, preventing communication between the CyberArk Identity Connector and the LDAP Server (A). This is a common issue where firewall settings prevent the secure communication port (typically 636 for LDAPS) from transmitting data between the server and the connector, thus blocking the connection attempt.

? 'Verify Server Certificate' is activated but the provided hostname is not listed as a Subject Alternative Name (SAN) in the LDAP server's certificate (C). This scenario occurs when SSL/TLS security measures are stringent, requiring that the hostname used to connect to the LDAP server must match one listed in the server's SSL certificate. If the hostname does not match, the connection will fail due to SSL certificate validation errors.

NEW QUESTION 25

What is a supported certificate format for retrieving the LDAPS certificate when not using the Cyberark provided LDAPS certificate tool?

- A. .der
- B. .p7b
- C. p7c
- D. p12

Answer: A

Explanation:

For retrieving the LDAPS certificate when not using the CyberArk provided LDAPS certificate tool, the supported certificate format is .der. The DER (Distinguished Encoding Rules) format is a binary form of a certificate rather than the ASCII PEM format. This format is widely supported across various systems for securing LDAP connections by providing a mechanism for LDAP servers to authenticate themselves to users. This information can be verified by checking LDAP configuration guides and CyberArk's secure implementation documentation which outline supported certificate formats for LDAP integrations.

NEW QUESTION 27

Which users are Privilege Cloud Standard built-in users? (Choose 2.)

- A. NASCorp
- B. saascorps
- C. CyberArkAdmin
- D. remoteAccessAppUser
- E. PASReporterUser

Answer: CE

Explanation:

In CyberArk Privilege Cloud Standard, certain users are predefined as built-in for administrative and operational purposes. The built-in users include:

? CyberArkAdmin (Option C): This user is typically set up as a default administrator with full access to manage and configure the Privilege Cloud environment.

? PASReporterUser (Option E): This user is often configured as a reporting user, designed to generate and access various reports without having broader administrative privileges.

Reference: CyberArk's Privilege Cloud setup and administration guides usually list these users as part of the default configuration to facilitate initial setup and ongoing management of the platform.

NEW QUESTION 31

What is the default username for the PSM for SSH maintenance user?

- A. proxymng
- B. psmmp_maintenance
- C. psmmpmaintenanceuser
- D. proxyusr

Answer: B

Explanation:

The default username for the Privileged Session Manager (PSM) for SSH maintenance user in CyberArk Privilege Cloud is psmmp_maintenance. This account is used for maintenance purposes and is integral for administrative tasks and configurations related to SSH sessions managed by the PSM. The username is predefined and standardized across deployments to maintain consistency and ensure security best practices are adhered to. The username is mentioned in the CyberArk official documentation regarding PSM configuration for SSH.

NEW QUESTION 35

What are the basic network requirements to deploy a CPM server?

- A. Port 1858 to the Privilege Cloud Vault service backend and Port 443 to the Privilege Cloud Portal
- B. Port 1858 only
- C. any ports to the Privilege Cloud Vault service backend
- D. Port UDP/1858 to the Privilege Cloud Vault service backend and all required ports to the targets and Port 3389 to the PSM

Answer: A

Explanation:

The basic network requirements to deploy a CyberArk Privilege Management Central Policy Manager (CPM) server include Port 1858 to the Privilege Cloud Vault service backend and Port 443 to the Privilege Cloud Portal. Port 1858 is necessary for communication with the CyberArk Vault, facilitating essential interactions like password retrieval and updates. Port 443 is required for secure web traffic to and from the Privilege Cloud Portal, ensuring that all management tasks performed through the web interface are secure and encrypted. These ports must be properly configured to allow for the efficient and secure operation of the CPM within the Privilege Cloud infrastructure.

NEW QUESTION 37

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

CPC-SEN Practice Exam Features:

- * CPC-SEN Questions and Answers Updated Frequently
- * CPC-SEN Practice Questions Verified by Expert Senior Certified Staff
- * CPC-SEN Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CPC-SEN Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CPC-SEN Practice Test Here](#)